Hyper-resolution principle, application to Nullstellensatz and bipartite graphs

Paolo Comensoli

03/04/2018

In the first two sections I will expand some details of the Lifschitz's paper Semantical completeness theorems in logic and algebra.¹ First of all I will briefly give the hyper-resolution principle and Robinson's theorem as stated by Lifschitz, then I will show the proof of Nullstellensatz with the aim to clarify every step. **Notation:**

- Literal: an atomic formula or a negation of an atomic formula.
- Clause: a finite set of literals.
- if Γ is a clause, $\overline{\Gamma}$ is the disjunction of the elements of Γ in a fixed order.

1 Hyper-resolution principle

Let T be a set of propositional formulae, each of the form:

$$\bigwedge_{i=1}^{m} A_i \to \bigvee_{j=1}^{n} B_j$$

Where the A_i 's and B_j 's are literals and m + n > 0.

We have the calculus H_T : the objects derivable are clauses and the rules of inference are:

$$\frac{\Gamma_1 \cup \{A_1\}, \cdots, \Gamma_m \cup \{A_m\}}{\Gamma_1 \cup \cdots \cup \Gamma_m \cup \{B_1, \cdots, B_n\}}$$
(1)

for every element of T. The formulae of the set T will be called the *non-logical* axioms of H_T

¹American Mathematical Society, Volume 79, Number 1, May 1980, Pages: 89-96

Example Let $T = \{A \to B \lor C, A, \neg B\}$, then H_T has three rules:

$$\begin{array}{ccc} \Gamma \cup \{A\} & \Gamma & \Gamma \cup \{B\} \\ \hline \Gamma \cup \{B,C\} & \Gamma \cup \{A\} & \Gamma \end{array}$$

Using such rules we get the tree:

$$\frac{\varnothing}{\{A\}}$$

$$\frac{\{B,C\}}{\{C\}}$$

and we write $\varnothing \vdash_{H_T} \{C\}$

Given a rule in the form (1) and an application of it in a derivation, whenever $A_i \in \Gamma_i$ for some i, we call such application trivial. The following two lemmas ensure that such kind of application can always be removed.

Lemma 1.1. Let Π be obtained from $\Sigma_1, ..., \Sigma_m$ by one application of a rule H_T . For any $\Sigma'_1 \subset \Sigma_1, ..., \Sigma'_m \subset \Sigma_m$, one of the two following holds:

- (a) $\Sigma_i' \subset \Pi$ for some i
- (b) some $\Pi' \subset \Pi$ can be obtained from $\Sigma'_1, ..., \Sigma'_m$ by an application of the same rule

Proof: Consider an application of (1) leading from $\Sigma_1, ..., \Sigma_m$ to Π , for this application:

$$\Sigma_1 = \Gamma_1 \cup \{A_1\}, ..., \Gamma_m \cup \{A_m\}$$

$$\Pi = \Gamma_1 \cup ... \cup \Gamma_m \cup \{B_1, ..., B_n\}$$

Consider the following two cases:

- (a) $A_i \notin \Sigma_i'$ form some i. Then $\Sigma_i' \subset \Gamma_i \subset \Pi$
- (b) $A_i \in \Sigma_i'$ for every i. Then $\Sigma_i' = \Gamma_i' \cup \{A_i\}$ where $\Gamma_i' = \Sigma_i' \setminus \{A_i\}$, one application of (1) to $\Sigma_1', ..., \Sigma_m'$ gives $\Pi' = \Gamma_1' \cup ... \cup \Gamma_m' \cup \{B_1, ..., B_n\} \subset \Pi$

Lemma 1.2. For every derivation of a clause Π in H_T there exists a derivation of some $\Pi' \subset \Pi$ in H_T without trivial application of rules of inference.

Theorem 1.3 (Robinson's, version 4). For any clauses $\Gamma_1, \dots, \Gamma_l, \Delta$, if in every model of T, the following is valid

$$\overline{\Gamma}_1 \wedge \cdots \wedge \overline{\Gamma}_l \to \overline{\Delta}$$

then there exists a derivation of some $\Delta' \subseteq \Delta$ from $\Gamma_1, \dots, \Gamma_l$ in H_T , containing no trivial application of rules of inference.

2 Nullstellensatz

Using Hyper-resolution principle and Robinson's theorem it is possible to prove the Nullstellensatz as stated here:

Let K be a field and $f, f_1, \dots, f_l \in K[\underline{x}]$, if in any extension of K, f vanishes at all common zeros of f_1, \dots, f_l , then there exists $p \in \mathbb{N}$ and $h_1, \dots, h_l \in K[\underline{x}]$ such that

$$f^p = \sum_{i=1}^l h_i \cdot f_i$$

To this aim, consider the first order language $\mathcal{L} = \{+, \cdot, =0\} \cup K$ where $+, \cdot$ are binary function symbols, = 0 is a unary predicate symbol and the elements of K are constants; so the terms are polynomials over K and the atomic formulae are algebraic equations.

Consider the theory given by the following axioms:

$$0 = 0 \tag{2}$$

$$\neg (1=0) \tag{3}$$

$$r_1 = 0 \rightarrow r_2 = 0$$
 $(r_1, r_2 \text{ are equal polynomials})$ (4)

$$(r = 0 \land s = 0) \to r + s = 0 \tag{5}$$

$$r = 0 \to r \cdot s = 0 \tag{6}$$

$$r \cdot s = 0 \to (r = 0 \lor s = 0) \tag{7}$$

One can prove the equality axioms, the axioms of integral domain and the diagram of K. It follows that the models of the theory are the integral domains that contains K. Lifschitz, instead of the axiom $\neg(1=0)$, uses the axioms $\neg(\alpha=0)$ for each $\alpha \in K \setminus \{0\}$, however the one taken here is equivalent and simplifies the next arguments.

The calculus H_T consists of the axiom $\{0=0\}$ and of the rules of inference:

$$\frac{\Gamma \cup \{1 = 0\}}{\Gamma} \tag{8}$$

$$\frac{\Gamma \cup \{r_1 = 0\}}{\Gamma \cup \{r_2 = 0\}} \qquad r_1, r_2 \text{ are equal polynomials} \tag{9}$$

$$\frac{\Gamma \cup \{r=0\}, \ \Delta \cup \{s=0\}}{\Gamma \cup \Delta \cup \{r+s=0\}}$$

$$(10)$$

$$\frac{\Gamma \cup \{r = 0\}}{\Gamma \cup \{r \cdot s = 0\}} \tag{11}$$

$$\frac{\Gamma \cup \{r \cdot s = 0\}}{\Gamma \cup \{r = 0, s = 0\}} \tag{12}$$

Note that the rules (8-11) do not increase the number of elements of the clauses, precisely for an application

$$\frac{\Gamma \Delta}{\Sigma}$$
 (8-11)

we have $|\Sigma| \leq |\Gamma \cup \Delta|$; while for rule (12) we have $\Delta = \emptyset$ and $|\Sigma| = |\Gamma| + 1$.

For any derivation in H_T there is a tree with all the applications of the rule (12) at the bottom; this is ensured by the following.

Lemma 2.1. Every derivation in H_T which contains non-trivial applications can be rearranged in such a way that any application of (12) is either the last one or it is followed by an application of (12).

Proof: Suppose to have a non-trivial application of a rule (12) followed by a rule (x) different from (12):

$$\frac{\Gamma \cup \{r \cdot s = 0\}}{\Gamma \cup \{r = 0, s = 0\},} 12 \Delta$$

$$\Sigma \cup \{r = 0, s = 0\}$$

Here Δ is the second premise in case (x) is the rule (10), otherwise it should be dropped. In the case that both r = 0 and s = 0 in the conclusion are different from A_1 shown in the scheme (1) of the rule (x), then $A_1 \in \Gamma$ and we can change the order as follow:

$$\frac{\Gamma \cup \{r \cdot s = 0\}, \quad \Delta}{\sum \cup \{r \cdot s = 0\}} x$$

$$\Sigma \cup \{r = 0, s = 0\}$$
12

Otherwise let $\{r = 0\}$ be A_1 of (x), depending on whether (x) is (8),(9), (10) or (11), change the derivation according to one of the schemes below

$$\frac{\Gamma \cup \{1 \cdot s = 0\}}{\Gamma \cup \{1 = 0, s = 0\}} 12$$

$$\Gamma \cup \{s = 0\}$$

$$8 \longrightarrow \frac{\Gamma \cup \{1 \cdot s = 0\}}{\Gamma \cup \{s = 0\}} 9$$

$$\frac{\Gamma \cup \{r_1 \cdot s = 0\}}{\Gamma \cup \{r_1 = 0, s = 0\}} 12 \qquad \frac{\Gamma \cup \{r_1 \cdot s = 0\}}{\Gamma \cup \{r_2 \cdot s = 0\}} 9 \\
\Gamma \cup \{r_2 = 0, s = 0\} \qquad \longrightarrow \qquad \Gamma \cup \{r_2 = 0, s = 0\}$$

$$\frac{\Gamma \cup \{r \cdot s = 0\}}{\Gamma \cup \{r = 0, s = 0\}} 12 \qquad \frac{\Gamma \cup \{r \cdot s = 0\}, \quad \Delta \cup \{t = 0\}}{\Delta \cup \{t \cdot s = 0\}} 10}{\Gamma \cup \Delta \cup \{r + t = 0, s = 0\}} 10 \qquad \Rightarrow \qquad \frac{\Gamma \cup \{r \cdot s = 0\}, \quad \Delta \cup \{t \cdot s = 0\}}{\Delta \cup \{t \cdot s = 0\}} 10}{\Gamma \cup \Delta \cup \{r + t = 0, s = 0\}} 12$$

$$\frac{\Gamma \cup \{r \cdot s = 0\}}{\Gamma \cup \{r \cdot s = 0\}} 12$$

$$\frac{\Gamma \cup \{r \cdot s = 0\}}{\Gamma \cup \{r \cdot t = 0, s = 0\}} 12$$

$$\frac{\Gamma \cup \{r \cdot s = 0\}}{\Gamma \cup \{(r \cdot s) \cdot t\}} 11$$

$$\Rightarrow \frac{\Gamma \cup \{r \cdot s = 0\}}{\Gamma \cup \{(r \cdot t) \cdot s = 0\}} 12$$

By a series of application of this procedure, we obtained a derivation as required.

Now we have all the tools to achieve the proof of nullstellentsatz:

Proof: Let K be a field and $f, f_1 \cdots f_l \in K[\underline{x}]$ such that in any extension of K, f vanishes at all common zeros of $f_1 \cdots f_l$. This amounts to require that in every model of (2-7) the following is valid:

$$\Gamma_1 \wedge \cdots \wedge \Gamma_l \to \Delta$$

where $\Gamma_i = \{f_i = 0\}$ and $\Delta = \{f = 0\}$.

Then by Robinson's theorem: $\Gamma_1, \dots, \Gamma_l \vdash_{H_T} \Delta'$ where either $\Delta' = \emptyset$ or $\Delta' = \{f = 0\}$. In particular take a derivation without trivial applications and where all the applications of (12) are at the bottom, the existence of such tree is ensured by the lemma shown above. The tree is of the form:

$$\frac{\Gamma_1, \dots, \Gamma_l}{\Sigma} 8-11$$

$$\vdots \text{ only rules } 12$$

$$\Delta' \tag{13}$$

Since all the Γ_i 's are singletons, and since the rules (8-11) do not increase the size of the clauses, Σ is either a singleton or the empty set. Let's treat separately the cases of Δ' .

Case
$$\Delta' = \emptyset$$

The only way to get \emptyset out of the rules of inference is by applying (8), in this case rule (12) does not apply at all and the tree is of the form:

$$\frac{\Gamma_1, \cdots, \Gamma_l}{\{1=0\}} 9 - 11$$

1 is obtained by a series of applications of rules (9 - 11), therefore it is a linear combination of f_1, \dots, f_l :

$$f^0 = 1 = \sum_{i=1}^{l} h_i \cdot f_i$$

Case
$$\Delta' = \{f = 0\}$$

Suppose that rule (12) applies p-1 times, (8) does not apply at all and the tree is of the form:

$$\frac{\Gamma_1, \cdots, \Gamma_l}{\Sigma} 9 - 11$$

$$\frac{\Gamma_1}{\{f = 0\}} (p - 1) \text{ applications of } 12$$

Since (12) applies and Σ is a singleton, Σ must be of the form $\{t_1 \cdot r_1 = 0\}$. Suppose that the A_1 of the i^{th} application is $r_i = t_{i+1} \cdot r_{i+1}$, then the tree is:

$$\frac{\Gamma_{1}, \cdots, \Gamma_{l}}{\{t_{1} \cdot r_{1} = 0\}} = 9 - 11$$

$$\frac{\{t_{1} \cdot r_{1} = 0\}}{\{t_{1} = 0, t_{2} \cdot r_{2} = 0\}} = 12$$

$$\vdots$$

$$\frac{\{t_{1} = 0, \cdots t_{p-2} = 0, t_{p-1} \cdot r_{p-1} = 0\}}{\{t_{1} = 0, \cdots, t_{p-1} = 0, r_{p-1} = 0\}} = 12$$

Since the root of the tree must be the singleton $\Delta' = \{f = 0\}$, it is the case that for any i: $t_i = r_{p-1} = f$. Therefore $\Sigma = \{f^p = 0\}$ and we conclude

$$f^p = \sum_{i=1}^l h_i \cdot f_i$$

3 Bipartite Graph

In this section I will show, using hyper-resolution, that a graph is bipartite if and only if it does not contain odd cycles. To do so, firstly I will give a brief recall on graph theory in order to fix notation and terminology. Then I will show the Matiyasevich's approach to describe colouring in hyper-resolution and I will use it to prove the characterization of bipartite graphs.

Recall on graph theory

A simple graph G is a couple of sets (V, E) such that the elements of E are unordered couples of elements of V. The elements of V are called *vertices* and the elements of E are called *edges*. A vertex V is *incident* with an edge E if E is one of the two elements of E, the two vertices incidents an edge are called its *ends* and are said to be *adjacent*; an edge whose endpoints are E and E is denoted as E and E is a subgraph of E if E is a subgraph of E is a subgraph of E if E is a subgr

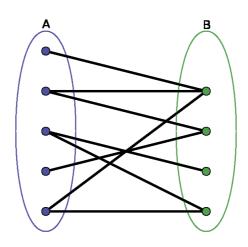
A path is a graph P = (V, E) of the form:

$$V = \{x_0, x_1, ..., x_n\}$$
 $E = \{x_0x_1, x_1x_2, ..., x_{n-1}x_n\}$

where the vertices are pairwise different, the length of the path is defined as the cardinality of E which is n. A *cycle* is a path where x_n coincides with x_0 ; a cycle of length n will be briefly called n-cycle; if a n-cycle is a subgraph of G, we say that G has a n-cycle.

A k-colouring of a graph G = (V, E) is a map $c : V \to \{1, ..., k\}$ such that $c(v) \neq c(w)$ whenever v and w are adjacent; a graph is k-colourable if it admits a k-colouring.

A graph G = (V, E) is bipartite if V admits a partition in two subsets such that every edge has its ends in different subsets; clearly a graph is bipartite if and only if it is 2-colourable.



Resolution approach

Every colouring can be uniquely described (up to renaming the colours) by the symmetric binary relation "vertices x and y have the same colour", which we denote by $\mathscr{E}xy$. Such binary relation, in order to represent a colouring map, should respect a transitivity axiom, and be false whenever the two vertices are adjacent

$$\mathscr{E}xy \wedge \mathscr{E}yz \to \mathscr{E}xz \tag{14}$$

$$(xy \in E \Rightarrow) \qquad \neg \mathscr{E}xy \tag{15}$$

Also for an *n*-colouring we require that whenever we pick n+1 vertices at least 2 of them must share the colour, which amount to require for any $\{x_0, x_1, ..., x_n\} \subseteq V$

$$\bigvee_{i=0}^{n-1} \bigvee_{j=i+1}^{n} \mathscr{E}x_i x_j \tag{16}$$

Conversely if a binary symbol satisfies the above axioms, then it corresponds to some colouring map. More formally, for every graph G = (V, E), we consider a language $\mathcal{L} = \{\mathcal{E}\} \cup V \cup E$, where \mathcal{E} is a binary relation symbols and $U \cup V$ are constants; the models of the formulae (14-16) are the n-colourable graphs that contain G, if G is not n-colourable the axioms are inconsistent and there are no models. The formulae (14-16) give rise to the calculus H_G which consists of the following inference rules:

$$\frac{\Gamma \cup \{\mathscr{E}xy\} \quad \Delta \cup \{\mathscr{E}yz\}}{\Gamma \cup \Delta \cup \{\mathscr{E}xz\}}$$

$$(17)$$

$$\frac{\Gamma \cup \{\mathscr{E}xy\}}{\Gamma} \quad xy \in E \tag{18}$$

$$\frac{\Gamma}{\Gamma \cup \{\mathscr{E}x_0x_1, ..., \mathscr{E}x_{n-1}x_n\}} \tag{19}$$

Note that any tree made with these rules have (19) as leaves; on the other hand, if there are no trivial applications, rule (19) appears only at leaves, indeed $\emptyset \in \Gamma$ for every non-empty Γ .

Proposition 3.1. A graph G = (V, E) that contains an odd cycle is not 2-colourable

I will show that if there is an odd cycle the empty clause is derivable in H_G , i.e. $\vdash_{H_G} \varnothing$, and that therefore the propositions (14-16) are inconsistent. Let $\{x_1,...,x_{2n+1}\}$ be an odd cycle, by definition for i=1,2,...,2n $x_ix_{i+1} \in E$ and $x_{2n+1}x_1 \in E$. Then consider the following deduction in H_G :

$$\frac{\mathscr{E}x_{1}x_{2}, \mathscr{E}x_{2}x_{3}, \mathscr{E}x_{1}x_{3}}{\mathscr{E}x_{2}x_{3}, \mathscr{E}x_{1}x_{3}}(18) \qquad \frac{\mathscr{E}x_{3}x_{5}, \mathscr{E}x_{4}x_{5}, \mathscr{E}x_{3}x_{5}}{\mathscr{E}x_{4}x_{5}, \mathscr{E}x_{3}x_{5}}(18) \qquad \qquad \frac{\mathscr{E}x_{2}x_{3}, \mathscr{E}x_{1}x_{3}}{\mathscr{E}x_{1}x_{3}}(18) \qquad \qquad \frac{\mathscr{E}x_{1}x_{5}}{\mathscr{E}x_{3}x_{5}}(17) \qquad \qquad \mathscr{E}x_{2}x_{2}x_{2}x_{2}x_{2}x_{2}x_{1}, \mathscr{E}x_{2}x_{2}x_{2}x_{1}}{\mathscr{E}x_{2}x_{2}x_{2}x_{2}x_{1}}(18) \qquad \qquad \frac{\mathscr{E}x_{2}x_{2}x_{2}x_{2}x_{2}x_{1}}{\mathscr{E}x_{2}x_{2}x_{2}x_{2}x_{2}x_{2}}(18) \qquad \qquad (18)$$

The idea shown by this tree is that, if the graph is 2-colourable with a (2n+1)-cycle and c is a 2-colouring map, whenever we pick three consecutive vertices x_i, x_{i+1}, x_{i+2} of the cycle, two of them must be of the same colour and since adjacent vertices have different colours, we have $c(x_i) = c(x_{i+2})$; whence $c(x_1) = c(x_3) = c(x_5) = \dots = c(x_{2n+1})$ which is a contradiction since $x_1x_{2n+1} \in E$. Before proving the opposite direction, we need the following result.

Lemma 3.2. Every derivation in H_G can be rearranged in such a way that any application of (18) is either the last one or it is followed by an application of (18).

Proof:

$$xy \in E \frac{\Gamma \cup \{\mathscr{E}xy, \mathscr{E}ab\}}{\Gamma \cup \{\mathscr{E}ab\}} 18 \xrightarrow{\Delta \cup \{\mathscr{E}bc\}} 17 \xrightarrow{xy \in E \frac{\Gamma \cup \Delta \cup \{\mathscr{E}xy, \mathscr{E}ab\}}{\Gamma \cup \Delta \cup \{\mathscr{E}ac\}}} 18} \xrightarrow{17}$$

Proposition 3.3. If a graph G = (V, E) is not 2-colourable, then it has an odd cycle

If G is not 2-colourable, also every graph that contains G is not 2-colourable; by Robinson's theorem and lemma 3.2, we know that $\vdash_{H_G} \varnothing$ and in particular there is a derivation without trivial application where all the applications of (18) are close to the root. Now we proceed by induction on the number k of application of (17). If k = 0 the tree is of the form:

$$\frac{ \{\mathscr{E}xy, \mathscr{E}yz, \mathscr{E}xz\}}{xz \in E} 19$$

$$\frac{ \{\mathscr{E}xy, \mathscr{E}yz\}}{xz \in E}$$

$$\frac{ \{\mathscr{E}xy\}}{\varnothing} xy \in E$$

Then $xy, xz, yz \in E$ and the 3-cycle $\{x, y, z, x\}$ is a subgraph of G.

For k > 0 the tree is of the form:

$$\begin{array}{ccc}
\varnothing & \varnothing \\
\vdots & \vdots \\
\Gamma \cup \{\mathscr{E}xy\} & \Delta \cup \{\mathscr{E}yz\} \\
\hline
\Sigma \cup \{\mathscr{E}xz\} \\
\vdots \\
\varnothing
\end{array}$$

Whence $xz \in E$ and if $\mathscr{E}ab \in \Gamma \cup \Delta$ then $ab \in E$.

Consider $E' = E \cup \{xy, yz\}$, the graph G' = (V, E') has G as subgraph, thus we have the following trees in H_G

$$\begin{array}{ccc}
\varnothing & \varnothing \\
\vdots & \vdots \\
\Gamma \cup \{\mathscr{E}xy\} \\
\Gamma & \Delta \cup \{\mathscr{E}yz\} \\
\hline
\Gamma & \Delta \\
\vdots & \Gamma \subseteq \Sigma
\end{array}$$

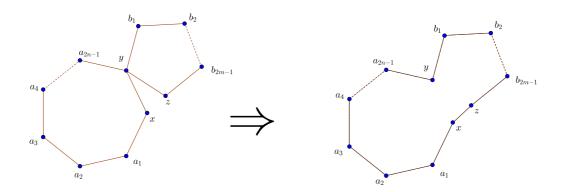
$$\begin{array}{ccc}
\varnothing & \vdots \\
\Delta \cup \{\mathscr{E}yz\} \\
\Delta & \vdots \\
\Delta \subseteq \Sigma$$

by induction hypothesis G' has two odd cycles C_1 and C_2 .

If $y \notin C_1$ (or C_2), then C_2 (or C_1) is an odd cycle of G.

Thus let $y \in C_1 \cap C_2$, if $x \notin C_1$ (or $y \notin C_2$), then C_2 (or C_1) is an odd cycle of G; so consider $x \in C_1$ and $z \in C_2$, if $x, z \in C_1 \cap C_2$, $\mathscr{E}yz \in \Gamma$ and $\mathscr{E}xy \in \Delta$ whence $\mathscr{E}yz, \mathscr{E}xy, \mathscr{E}xz \in \Sigma \cup \{\mathscr{E}xz\}$ and G has the cycle $\{x, y, z, x\}$.

The last case to be considered is $y \in C_1 \cap C_2$, $x \in C_1 \setminus C_2$, $z \in C_2 \setminus C_1$; let 2n + 1 and 2m + 1 respectively the length of C_1 and C_2 , if y is the only vertex in the intersection, by removing the edges xy, yz and adding xz we get a cycle in G of length 2(n + m) + 1.



It remains to consider when C_1 and C_2 intersect multiple times, let P and Q be the longest path respectively of C_1 and C_2 with $y \in P \cap Q$ and where the only vertices that belong to $C_1 \cap C_2$ are the endpoints of the paths. Then $P \cup Q$ is a cycle that pass trough the edges xy and yz, if the length of such cycle is even, by removing xy, yz and adding xz we get an odd cycle in G.

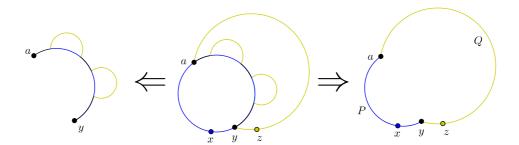


Figure 1: In blue $C_1 \setminus C_2$, in yellow $C_2 \setminus C_1$ and in black the intersection

If $P \cup Q$ is an odd cycle, consider the remaining part which namely consists of $C_1 \cap C_2$ and of $\tilde{C}_1, ..., \tilde{C}_l$ cycles, then at at least one of them must be odd since $|P \cup Q|$ is odd and the following holds

$$2n + 1 + 2m + 1 - |P \cup Q| = \sum_{i=1}^{l} length(\tilde{C}_i) + 2 \cdot |C_1 \cap C_2|$$

Finally, since $xy \in P$ and $yz \in Q$, such odd cycle is also in G.